AISOM
Associazione Nazionale delle Imprese

COMUNICATO

Martedì 24 maggio 2022 si è tenuto il **webinar**
patrocinato da **AISOM**, **AICIM**, **AIMBA** e **OIERRE**

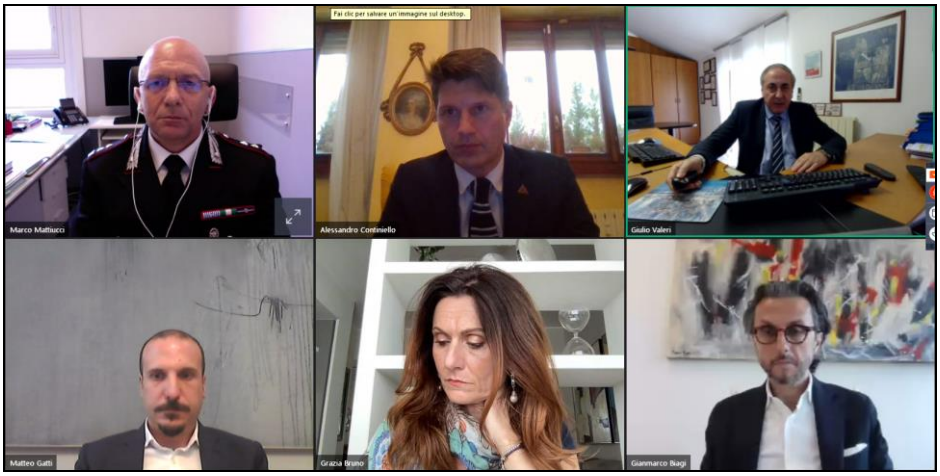
Prospettive per l'economia italiana tra vincoli da dazi, sanzioni economiche e rischi informatici

L'evento è stato un importante momento di confronto sulle inevitabili conseguenze geopolitiche ed economiche che la guerra tra Russia e Ucraina sta provocando in termini di crescita, commerci, inflazione e **sicurezza informatica**. In questo scenario incerto, stanno infatti emergendo le debolezze strutturali di un'economia globale fortemente impattata da tematiche quali l'interruzione delle catene di approvvigionamento o la crisi delle materie prime. **Il webinar ha voluto dare risposte in merito a come le imprese italiane devono affrontare queste nuove sfide** per gestire al meglio il proprio business e quali **investimenti strutturali** e in **risorse umane** devono prevedere per rispondere adeguatamente ad un contesto di mercato delicato e pieno di rischi.

E' stato *chairman* e coordinatore dell'evento **Giulio Valeri**, Membro del Consiglio Direttivo Nazionale AISOM e CEO di **Software Solutions** (Azienda specializzata in analisi e soluzioni per la cyber sicurezza).

Le continue minacce e ritorsioni da parte del governo russo alla partecipazione italiana alle sanzioni applicate dai paesi UE e NATO e l'invio di armi e assistenza in Ucraina, per contrastare l'avanzata militare russa, hanno generato una crescita esponenziale di attacchi informatici ad aziende pubbliche e private italiane da parte di hacker dell'est Europa. Per diversi motivi il governo russo non può adottare una guerra "convenzionale" e quindi per controbattere alle sanzioni economiche (parte italiana) ha nella guerra cibernetica lo strumento principe. Affossare l'economia italiana significa combattere ed abbattere i sistemi informatici di aziende pubbliche e private italiane, sia del mondo militare che in quello civile. Le contromosse delle aziende italiane devono necessariamente partire dalla protezione dei propri asset informatici, ogni azienda, di qualsiasi settore economico e dimensione deve cambiare la strategia della propria sicurezza informatica.

Tutti i relatori coinvolti hanno apportato interessanti spunti di riflessione.



Il **Ten. Col. Marco Mattiucci**, Capo del Centro Sicurezza Telematica del Comando Generale – **Arma dei Carabinieri -** nel suo intervento "*L'emergente nuovo modello di cybersecurity quale elemento trasversale e unificatore in ambito istituzionale e privato"* ha sottolineato come l'Arma dei Carabinieri è in prima fila non solo per la prevenzione delle proprie strutture (SOC) ma anche per fungere da consulente a tutti i servizi pubblici che devono essere protetti dall'accrescersi degli attacchi e dai rischi di fermo sistemi se non addirittura dalla devastazione di lungo periodo della funzionalità dei sistemi. Il precedente leit motiv "hackeraggio per finalità di ricatto economico" è stato sorpassato dalla volontà ed obiettivo di costringere l'economia delle aziende a fermarsi per il maggior tempo possibile: sia sistemi proprietari, sia sistemi appoggiati a cloud systems, sia sistemi basati su reti di PC che sistemi di telefonia mobile dove sempre più spesso risiedono applicazioni vitali di comunicazione tra aziende e le proprie risorse, i clienti ed i fornitori.

L'**Ing. Gianmarco Biagi**, Presidente AICIM, Membro del Consiglio Direttivo Nazionale AISOM e Presidente di SettePuntoNove Holding – ha presentato il suo contributo "*I limiti attuali della cultura imprenditoriale italiana nell'information risk*" descrivendo le linee guida di come le PMI (grande risorsa per il rilancio del Paese) debbano trovare, soprattutto in questo memento storico, la capacità di pensare, formalizzare ed attuare un Piano industriale di rilancio della propria Impresa, basato su: apertura del capitale, crescita dimensionale anche per aggregazioni, internazionalizzazione, management dedicato e altamente skillato, digitalizzazione.
Ponendo poi particolare attenzione alla parte relativa alla digitalizzazione, Biagi pone l'accento sulla parte del piano industriale dedicata alla digitalizzazione stessa, che comprende la capacità dell'impresa di sviluppare il proprio business ed efficientare i processi tramite le nuove Tecnologie Abilitanti, tra le altre realtà virtuale, realtà aumentata, Intelligenza Artificiale, indicando come le grandi imprese stanno da tempo investendo in questa direzione con risultati ottimi. Parte di questo processo è senza dubbia la protezione e la Cyber Security che, sovente, "snobbata" dalle PMI. Spesso l'imprenditore si sente sicuro perché ha fatto qualche investimento nei 3-5 anni precedenti con qualche accorgimento tecnico ed organizzativo, con l'acquisto di qualche prodotto software. Mediamente l'imprenditore sottovalutata come siano cambiati gli scenari (dal ricatto appunto alla distruzione) ma soprattutto come la necessità di protezione debba evolversi con l'evolversi delle tecnologie, al fine di evitare la perdita parziale ed a volte integrale degli investimenti prodotti in Azienda. Contrastare l'hackeraggio sempre più mirato e pericoloso significa pensare domani a destinare attenzioni, soluzioni e budget costanti e non più investimenti una tantum. Per l'imprenditore è un errore strategico enorme non considerare la digitalizzazione e la cyber come partner del proprio business.

Matteo Gatti, Unit Manager Milano di **Mentor & Faber** – (Società specializzata in head hunting di middle management ed executive e nella consulenza aziendale organizzativa e commerciale) è intervenuto in merito a "*La domanda crescente di figure specializzate in guerra informatica, sicurezza IT"* confermando che negli ultimi mesi, ed in particolare dall'inizio del conflitto russo – ucraino, la richiesta di profili sempre più skillati nell'ICT è accresciuto fino a diventare uno degli ambiti professionali più ricercati dalle figure di ICT Management; ora l'interesse si è spostato proprio su figure che conoscono le problematiche di cyber security. Anche se l'uso di consulenti è altrettanto accresciuto, proprio la necessità di tenere costantemente sotto controllo gli attacchi e adeguare le misure tecnico – organizzative richiede una presenza sia di livello superiore sia una presenza di lungo periodo. Spesso gli imprenditori non hanno la possibilità di conoscere l'evoluzione tecnologica, di conoscere la profondità della formazione e delle esperienze dei soggetti di cui sono alla ricerca e quindi l'assistenza di una società specializzata in tali attività diventa strategica per individuare e selezionare profili rispondenti a requisiti necessari.

L'**Avv.to Alessandro Continiello**, Capo Divisione Ethics & Compliance dello **Studio Legale Martinez & Novebaci** ha esposto "*I rischi delle aziende verso i clienti e i fornitori in questo nuovo scenario di guerra cibernetica"* puntualizzando che una delle prime cose che è balzata agli occhi delle aziende colpite da hackeraggio di ultima generazione è proprio la questione legale legata ai livelli di servizio e ai danni che gli hackeraggi possono costituire tra imprese, clienti e fornitori. Imprese che non ricevono ordini di fornitura non possono consegnare prodotti od organizzare al meglio i servizi. La mancata o parziale fatturazione può creare difficoltà finanziarie e danni per il mancato pagamento di tasse con il conseguente aggravio di ulteriori oneri. Una attenta analisi sulle indisponibilità nel tempo dei problemi causati da hackeraggi (e le ripartenze anche in down grade del sistema connettivo aziendale) dovrebbero consentire ad ogni impresa, indipendentemente dalle dimensioni ed attività, una valutazione dei rischi, dei costi finanziari (e non) e dell'indisponibilità delle informazioni. Altro aspetto critico, soprattutto per la legislazione internazionale, è la sottrazione di database di nomi, indirizzi inseriti nei propri archivi. La sottrazione di database nominativi è un punto sanzionabile per il Regolamento UE 679/16 e ha un costo molto alto. La sicurezza informatica viene ancora spesso vista come un costo: ma il vero costo invece è quello giuridico ed economico, in caso di attacchi, sia per l'impresa che per le sue figure apicali.

Grazia Bruno, Direttore Operativo **Expandi IT** (Società di intermediazione assicurativa esperta in tematiche legate al Cyber Risk) infine ha esposto "*Come garantire alle aziende la continuità in caso di criticità"* rimarcando che se le attività e le strategie preventive possono essere di sicuro un deterrente a valle, per diminuire i rilievi di rischiosità e le reiterazioni dei reati subiti, le aziende devono rendersi conto che ci sono anche strumenti (a monte) di gestione delle criticità laddove emersi i problemi. Alla data, uno strumento di risk management è rappresentato da possibili polizze assicurative che – opportunamente dimensionate dopo una analisi della "rischiosità" – possono consentire ad una azienda di avere le spalle coperte nella situazione spiacevole di dover assumere costi imprevisti – sia hardware che software che di servizi consulenziali - a supporto della ricostruzione dei dati e pagamento di penali verso clienti. Spesso la crescita degli attacchi e l'alta probabilità di rischio su più fronti (operativo, logistico, dati), non viene ancora percepito come reale e tangibile. In molti casi la protezione assicurativa è la variabile che consente di superare o mitigare l'attacco, anche in termini di servizi di assistenza operativa sia sul fronte tecnico, che su quello legale e della comunicazione.